

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

The person of Daniel Phillip Heintz, DOB 09/09/82, and any  
computers/digital media located thereon

Case No. 2:21-mj-93

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT C INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. 2251(d)	Advertising for child pornography
18 U.S.C. 2252 and 2252A	Possession, distribution, and/or receipt of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*[Handwritten signature]*

Applicant's signature

Brett M. Peachey, TFOFB

Printed name and title

Sworn to before me and signed in my presence.

Date: 2-10-21

City and state: Columbus, Ohio

*[Handwritten signature]*

Judge's signature

Chelsey M. Vascara, U.S. Magistrate Judge

Printed name and title



**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
EASTERN DIVISION**

<b>In the Matter of the Search of:</b>	)	No.
	)	
<b>The person of Daniel Phillip Heintz,</b>	)	<b>Magistrate Judge</b>
<b>DOB 09/09/82, the residence located at 6116 Myron</b>	)	
<b>Street Columbus, OH 43213, and any digital media</b>	)	
<b>located thereon/therein</b>	)	

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI),  
being duly sworn, hereby depose and state:

**I.     INTRODUCTION AND AGENT BACKGROUND**

1. TFO Brett M. Peachey, have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Child Exploitation and Human Trafficking Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children, including child pornography offenses and the online exploitation of children.
2. During my career as a Criminal Investigator and TFO, I have participated in various investigations of computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Criminal Investigator and task force officer, I investigate criminal violations relating to child exploitation and child pornography including the online enticement of minors and the illegal distribution, transmission, receipt, possession, and production of child pornography, in violation of 18 U.S.C. §§ 2252, 2252A, 2251 and 2422.
3. As a task force officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

**II.    PURPOSE OF THE AFFIDAVIT**

4. The facts and statements set forth in this affidavit are based on my knowledge, experience, and investigation, as well as the knowledge, experience, and investigative findings of others with whom I have had communications about this investigation, including other law enforcement officers and agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause for a search warrant for the person of Daniel Phillip HEINTZ (the SUBJECT PERSON) and the residence located at 6116 Myron Street Columbus OH 43213 (the SUBJECT PREMISES). I have not omitted any facts that would negate probable cause.
5. The SUBJECT PERSON and SUBJECT PREMISES to be searched are more particularly described in Attachment A and Attachment B respectively, for the items specified in Attachment C, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – the advertising of/for, distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the SUBJECT PERSON and the entire SUBJECT PREMISES, including the residential dwelling, curtilage, detached buildings and storage units, for any computers, cellular “smart” phones and/or mobile computing device or digital media located thereon/therein, and to thereafter seize and examine any such device that is recovered from the SUBJECT PERSON or SUBJECT PREMISES, for items specified in Attachment C, and to seize all items listed in Attachment C as evidence, fruits, and instrumentalities of the above violations.

### **III. APPLICABLE STATUTES AND DEFINITIONS**

6. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or if the notice or advertisement actually was transported using any means or facility

of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or commerce or is in or affecting interstate commerce.
8. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
9. As it is used in 18 U.S.C. §§ 2251 and 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.
10. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”<sup>1</sup> is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer

---

<sup>1</sup> The term child pornography is used throughout this affidavit. All references to this term in this affidavit and all Attachments hereto include both visual depictions of minors engaged in sexually explicit conduct as



generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

11. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.
12. The term “minor”, as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as “any person under the age of eighteen years.”
13. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.”
14. The term “visual depiction,” as used herein, is defined pursuant to 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
15. The term “computer”<sup>2</sup> is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
16. “Cellular telephone” or “cell phone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,”

---

referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

<sup>2</sup> The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

#### **IV. BACKGROUND REGARDING THE INTERNET AND MOBILE APPLICATIONS**

17. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
18. Computers, mobile devices, and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
19. Computers, tablets, and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a hard copy photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or

"JPG/JPEG" (Joint Photographic Experts Group) files.

20. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

21. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 128 Gigabytes. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 32 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 32 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic

storage devices is it possible to recreate the evidence trail.

22. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.
23. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.
24. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other



digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person “deletes” a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

25. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.
26. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
27. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment C.
28. A growing phenomenon related to smartphones and other mobile computing devices is the

use of mobile applications. Mobile applications, also referred to as “apps,” are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such “apps” include LiveMe, KIK messenger service, Snapchat, Meet24, and Instagram. Kik is a free mobile application that can be downloaded on Android or iOS devices that permits users to communicate anonymously with fellow Kik users. This application allows users to create groups where like-minded individuals can chat/text other users and post videos/images which includes groups in the sexual exploitation of children. Kik allows each user to create a unique username for their individual account when registering for the app. The username is a unique identifier that is tied to the individual’s Kik account that cannot be changed or replicated in any way. The only way for a registered user to create a new username is to shut down their Kik account and set up a new one with a different username. Kik also allows each user to create a display name. The display name is what the user shows publicly to connect with other registered Kik users. The display name can be changed at any time by the person who registered for the Kik account.

#### **V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

29. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- A. Computer storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
- B. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of

computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

30. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).
31. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices (including internal storage such as SD cards), any monitors, keyboards, and/or modems are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, and 2252A and should all be seized as such.

## **VI. SEARCH METHODOLOGY TO BE EMPLOYED**

32. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
  - a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment C;
  - b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment C;
  - c. Surveying various files, directories and the individual files they contain;

- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment C; and/or
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment C.

## VII. INVESTIGATION AND PROBABLE CAUSE

33. On August 28, 2020, a subject was arrested by the FBI in Illinois for attempted enticement of a minor, based on the subject's communications with and attempts to meet and engage in sexual activity with an undercover investigator posing as a 15-year-old female. The subject subsequently gave consent for investigators to assume his online identity for his Kik messaging account.
34. A review by FBI Illinois agents of the subject's previous Kik messages in his account revealed a conversation between the subject and an individual utilizing the Kik user name "hooah99," later identified as Daniel Heintz. In the conversations, which occurred in mid-August 2020, the Illinois subject and Heintz discussed their mutual sexual interest in children, and the possibility of Heintz taking a nude photo of [REDACTED]. They also exchanged images of themselves and files of pornography, including child pornography. The following is an excerpt of their conversation on August 9, 2020:

Illinois Subject:	When is [REDACTED] going to be home
Heintz:	In the morning
Heintz:	Unfortunately
Illinois Subject:	Really that sucks
Heintz:	I masturbated into a pair of her panties last night
Illinois Subject:	I want to see her pussy u ever see her naked
Heintz:	Occasionally. Not as much as I used to
Illinois Subject:	U ever take pictures
Heintz:	I'm gonna have to. Maybe while she's sleeping.
Heintz:	I've jerked off in her sleep before
Illinois Subject:	I want to watch that
Heintz:	You have anything else
Heintz:	I'd let you jerk of [sic] on her too. That could be fun.
Heintz:	Fuck I'm so horny
Illinois Subject:	Me to I want to lick [REDACTED] pussy
Heintz:	I'd love to watch you
Heintz:	I'd jerk off while you did



Illinois Subject: Where are you from just asking  
Heintz: Ohio  
Heintz: You?  
Heintz: Any more vidoes? I'm jerking off. What else you wanna do to [REDACTED]. Tell me everything.  
Illinois Subject: Fuck her till she can walk straight  
Heintz: Tell me about it.  
Illinois Subject: I'd rather show you  
Heintz: Help me cum  
Heintz: Any more videos? Or pictures

The Illinois subject then sent a photo of a female, approximately 13 to 14 years old, nude from the waist up.

Heintz: I love her tits  
Hetinz: I wanna cum on them

Heintz then sent a photo of a female, approximately twelve years of age, in a bathing suit on a beach.

Illinois Subject: Is that [REDACTED]  
Heintz: Yes  
Brinkley: Love her pussy very flexible

35. The conversation between the Illinois subject and Heintz continued over the next several days, during which the Illinois subject repeatedly requested photos of Heintz's and Heintz requested files of child pornography from the subject. The following is an excerpt of their conversation on August 12, 2020:

Illinois Subject: When u goin to be home  
Heintz: 315  
Heintz: Damn she's hot as fuck  
Illinois Subject: What time is it  
Heintz: 145  
Illinois Subject: Oh ok  
Illinois Subject: So in about a hour and half I'll get a live picture of her  
Heintz: Yes sir  
Illinois Subject: Ok

Heintz then sent a photo of a clothed female, approximately 12 to 13 years of age, smiling and seated on the floor. The photo appeared to be the same female that Heintz sent a photo of earlier in a bathing suit, which he stated was [REDACTED]

Illinois Subject: Thanks. Have you fucked her yet  
Heintz: I wish  
Heintz: I beat off to it a lot  
Illinois Subject: You see her naked  
Heintz: Sometimes  
Heintz: I see the 7 yr old more

Illinois Subject: Where is she now?  
Heintz: Upstairs  
Illinois Subject: Doing  
Heintz: Playing on her iPad  
Heintz: Do I get anything special for the live pic?  
Heintz: [REDACTED] will be back tomorrow and [REDACTED] in bed  
Illinois Subject: Who is picture of  
Heintz: [REDACTED]  
Heintz: 12  
Illinois Subject: How old is [REDACTED]  
Heintz: 7  
Illinois Subject: Nice  
Heintz: [REDACTED] is 7 too  
Illinois Subject: I try to send u something  
Illinois Subject: Can I see the 12 year old naked  
Illinois Subject: Yes I do like it. I'll have to take a naked one  
Illinois Subject: Please do.

36. Heintz and the Illinois subject continued their conversation the following day. Below is an excerpt of that conversation:

Illinois Subject: I want to see [REDACTED] pussy  
Heintz: I'd love to watch you rape her  
Illinois Subject: Which one  
Heintz: Either  
Heintz: Hell. Or [REDACTED]  
Illinois Subject: U goin to jack coffin her tonight  
Heintz: I could  
Illinois Subject: I would want to watch or see  
Heintz: I'd do that for you  
Heintz: Will you seen me a couple things to beat off to. Please  
Illinois Subject: Ya

The Illinois subject then sent a video depicting a nude female, approximately 13 to 15 years of age, masturbating and inserting an object in her anus. The female had some pubic hair but very minimal breast development.

Heintz: Mmmm. Please daddy  
Illinois Subject: Sending  
Heintz: Mmmmm  
Heintz: Fuck

The Illinois subject then sent another video depicting a nude female, approximately 13 to 15 years of age, masturbating with a hairbrush. The female does not have any pubic hair and very minimal breast development.

Heintz: I wanna fuck that little girl's pussy  
Heintz: Taste it  
Illinois Subject: What time do you think u will take the video and pics

Heintz: Whenever she goes to bed  
Heintz: I will take it for you  
Heintz: I want to make you happy  
Heintz: Please send some more. Any little boys?  
Illinois Subject: Thanks  
Heintz: I'm close to cumming  
Heintz: Please

37. Further information provided by SA Kurt Bendoraitis of the Springfield, IL office of the FBI stated that an undercover investigator messaged Heintz while utilizing the Illinois subject's Kik account on December 31, 2020, asking if Heintz had ejaculated on [REDACTED] [REDACTED] Heintz replied that he did while she was sleeping and took a photo of it but did not save it because he was worried due to the fact that his wife found a video of bestiality on his phone a month earlier.

38. On January 2, 2021, Kik responded to an emergency disclosure request for account information for "hooh99" with the following information:

Email Address: bigdan57@aol.com  
Model Phone: Iphone  
Registration Date: June 13, 2018 at 14:12:07 UTC  
IP Address: 23.125.33.29 on December 31, 2020 at 17:04  
UTC and January 1, 2021 at 16:23:42 UTC

39. IP address 23.125.33.29 is resolved to AT&T. An administrative subpoena was served on AT&T requesting subscriber information for IP address 23.125.33.29 for the two above dates and they responded with the following information:

Name: Jennifer Johnson  
Service/Billing Address: 6116 Myron Street, Columbus, OH 43213  
Billing Email: danielheintz@att.net  
Telephone Number: 614-738-3968

40. Open source database checks were conducted for the address information reported by AT&T, which revealed that a Jennifer Heintz (Johnson) and Daniel Heintz reside at 6116 Myron Street, Columbus, OH. A search of the Ohio Law Enforcement Gateway (OHLEG) revealed that both Jennifer Heintz and Daniel Heintz have valid driver's licenses with an address listed as the SUBJECT PREMISES. In addition, a review of Daniel Heintz's most recent OHLEG photo revealed that he is the same person depicted in a photo that was sent from the "hooh99" Kik account to the Illinois subject during a conversation on August 8,

2020.

41. A review of Jennifer Heintz's Facebook page revealed a group photo posted on January 25, 2020 that depicted herself, Daniel Heintz, two juvenile males and two juvenile females. One of the females in the photo appears to be the same female that Heintz sent photos of on two occasions to the Illinois subject during their Kik conversations.
42. During the course of this investigation, it was learned that Heintz is employed as a deputy with the Franklin County Sheriff's Office and is currently assigned to work at a jail operated by the Sheriff's Office. For safety concerns the warrant for the SUBJECT PERSON will be executed while the SUBJECT PERSON is at work in the Franklin County Sheriff's Office jail where he is assigned. Based on information obtained from other members of the Franklin County Sheriff's Office, your affiant believes that Heintz is likely to have his cellular phone on his person at that time. The warrant for the SUBJECT PREMISES will be executed after agents have made contact with the SUBJECT PERSON at the jail.

**VII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN**

43. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved seeking/soliciting, receiving, distributing, and/or collecting child pornography:
  - A. Those who seek out, exchange and/or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.
  - B. Those who seek out, trade and/or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may



use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Those who seek out, trade and/or collect child pornography sometimes maintain hard copies of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

D. Those who seek out, trade and/or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and have been known to maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

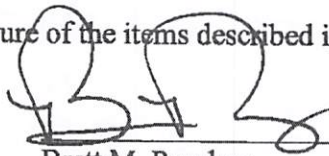
E. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

44. Based upon the conduct of individuals involved in seeking/soliciting, receiving, distributing, and/or collecting child pornography set forth in the above paragraphs, and the facts learned during the investigation in this case, namely, that Daniel Phillip HEINTZ has requested and received videos depicting child pornography via the Kik messenger app and has discussed engaging in sexual acts with [REDACTED] your affiant has reason to

believe that HEINTZ has a sexual interest in minors and has viewed or sought out visual depictions of minors engaged in sexually explicit conduct utilizing an internet-capable device, which may include a cellular phone that HEINTZ likely carries on his person. Furthermore, based on the information about HEINTZ's conduct contained herein, your affiant has reason to believe that HEINTZ has a sexual interest in minors and is an individual involved in seeking/soliciting, receiving, distributing, and/or collecting child pornography, and all of the characteristics of such individuals that are described above may be applicable. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of advertising for child pornography and distributing, receiving and possessing child pornography will be located on the SUBJECT PERSON and/or in the SUBJECT PREMISES and any digital device that may be found on/in the SUBJECT PERSON or the SUBJECT PREMISES.

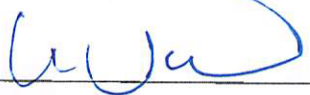
**IX. CONCLUSION**

45. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2251, 2252, and 2252A have been committed, and evidence of those violations is located on the SUBJECT PERSON, as more fully described in Attachment A, and within the SUBJECT PREMISES, as more fully described in Attachment B. Your affiant respectfully requests that the Court issue search warrants authorizing the search of the SUBJECT PERSON and the SUBJECT PREMISES and seizure of the items described in Attachment C.



Brett M. Peachey  
Task Force Officer  
Federal Bureau of Investigation

Sworn to and subscribed before me this 10 day of February 2021.



Chelsey M. Vascara  
United States Magistrate Judge  
United States District Court  
Southern District of Ohio

**ATTACHMENT A  
PERSON TO BE SEARCHED**

The subject person, Daniel Phillip HEINTZ, who is pictured below, DOB 09/09/82, is described as a Caucasian male, standing six feet, one inch tall and weighing approximately 255 pounds. This search warrant authorizes the search of HEINTZ for the items listed in Attachment C.





**ATTACHMENT B**  
**DESCRIPTION OF PLACE TO BE SEARCHED**

The place to be searched is the residence described below, including all its appurtenances, parking areas, outdoor working areas, detached buildings, and any computing related devices or digital media located therein.

6116 Myron Street Columbus, OH 43213 is described as a two-story single-family residence with dark tan siding, tan brick, black shutters, white trim and a two-car attached garage with white garage door. The number "6116" is affixed above the garage and on a mailbox across from the residence.





**ATTACHMENT C**  
**LIST OF ITEMS TO BE SEIZED**

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, USB/thumb drives, SD cards, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files, web cache information and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer for the purpose of distributing or receiving child pornography.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography.
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about

child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.

11. Any and all cameras, film, videotapes or other photographic equipment.

12. Any and all visual depictions of minors, whether clothed or not, for comparison to and identification of any child pornography images or videos discovered.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography.

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the residence of the person described in Attachment B.

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.